

## CLAIMS

We claim:

1    1. A method of generating an encrypted code in base L, comprising steps  
2    providing an n-bit raw number;

3               applying a one-way hash function on the n-bit raw number with a first secret  
4    key to generate a first string;

5               designating an m-bit portion of the first string as an m-bit validation number;  
6    and

7               combining the m-bit validation number and the n-bit raw number to generate  
8    a second string.

1    2. The method of claim 1, further comprising the steps of:

2               applying a DES3 encryption algorithm to the second string with a second  
3    secret key to generate a third string; and

4               converting the third string to base L to generate the encrypted code.

1    3. The method of claim 1, wherein n=32, m=16, and L=29.

1    4. The method of claim 1, wherein the one-way hash function is MD5.

1    5. The method of claim 1, wherein the step of combining includes  
2    concatenating the m-bit validation number and the n-bit raw number.

1    6. The method of claim 1, wherein the m-bit validation number is the m most  
2    significant bit (MSB) portion of the second string.

1    7. The method of claim 1, wherein the m-bit validation number is the m most  
2    significant bit (MSB) of the first string.

1    8. A method of verifying the validity of a code, comprising the steps of:  
2    generating a code with encrypted information;

81504.1.17

3           fixing the code on an object to be distributed to a user;  
4           obtaining the code from the object, by the user;  
5           receiving the code on line from the user;  
6           verifying the validity of the code by processing the encrypted information.

1     9.       The method of claim 8, wherein the step of generating includes the steps of:  
2               providing an n-bit raw number;  
3               applying a one-way hash function on the n-bit raw number with a  
4       first secret key to generate a first string;  
5               designating a m-bit portion of the first string as an m-bit validation  
6       number;  
7               combining the m-bit validation number and the n-bit raw number to  
8       generate a second string;  
9               applying a DES3 encryption algorithm to the second string with a  
10      second secret key to generate a third string; and  
11               converting the third string to a base L to generate the code with the  
12      encrypted information.

1     10.      The method of claim 9, wherein the step of verifying includes the steps of:  
2               converting the code in base L to generate a first test code in base 2;  
3               decrypting the first test code with the second secret key using a  
4       reverse DES3 encryption algorithm to generate a second test code;  
5               applying the one-way hash algorithm to the second test code to  
6       generate a third test code; and  
7               comparing a designated m-bit portion of the second test code to a  
8       designated m-bit portion of the third test code, and if the comparison is positive,  
9       declaring the code to be valid.

1     11.      The method of claim 10, wherein the m-bit validation number is the m-most  
2       significant bit (MSB) of the first string in the generating step and the designated m-  
3       bit portion is the most significant bit portion of the second test code in the  
4       comparing step.

1       12. A method for awarding incentive points to a user, comprising the steps of:  
2           generating a code with encrypted information;  
3           providing the code to an entity for printing on an object;  
4           receiving the code from a user on line, the code having been reterived from  
5   the object by the user;  
6           verifying the validity of the code by processing the encrypted information.

1       13. The method of claim 12, wherein the step of generating includes the steps  
2   of:  
3           providing an n-bit raw number;  
4           applying a one-way hash function on the en-bit raw number with a  
5   first secret key to generate a first string;  
6           designating an m-bit portion of the first string as an m-bit validation  
7   number;  
8           combining the m-bit validation number and the n-bit raw number to  
9   generate a scond string;  
10          applying a DES3 encryption algorithm to the second string with a  
11   second secret key to generate a third string; and  
12          converting the third string to base L to generate ateh code with the  
13   encrypted information.

1       14. The method of claim 13, wherein the step of verifying includes:  
2           converting the code in base L to generate a first test code in base 2;  
3           decrypting the first test code with the second secret key using a reverse  
4   DES3 encryption algorithm to generate a second test code;  
5           applying the one-way hash algorithm to the second test code to generate a  
6   third test code; and  
7           comparing a designated m-bit portion of the second test code to a designated  
8   m-bit portion of the third test code, and if the comparison is positive, declaring the  
9   code to be valid.

1    15.    The method of claim 14, wherein the step of verifying includes the steps of:  
2                 converting the code in base L to generate a first test code in base 2;  
3                 decrypting the first test code with the second secret key using reverse  
4                 DES3 encryption algorithm to generate a second test code;  
5                 applying the one-way hash algorithm to the second test code to  
6                 generate a third test code; and  
7                 comparing a designated m-bit portion of the second test code to a  
8                 designated m-bit portion of the third test code, and if the comparison is positive,  
9                 declaring the code to be valid.

1    16.    The method of claim 15, wherein the m-bit validation number is the m most  
2                 significant bit (MSB) of the first string in the generating step and the designated m-  
3                 bit portion is the most significant bit portion of the second test code and third test  
4                 code in the comparing step.

1    17.    An offline-online points system, comprising:  
2                 a main server configured for providing a user with an interface to submit a  
3                 code, wherein the code is obtainable offline and is associated with N points,  
4                 wherein each point, characterized as a purchase or attention incentive point, is  
5                 redeemable and maintainable in an account for the user;  
6                 a code server configured for maintaining valid codes and verifying, against  
7                 the valid codes, that the code submitted by the user is valid such that a balance in  
8                 the account for the user is increased by a predetermined number of points if the  
9                 code is valid;  
10                means for generating the code; and  
11                means for fixing the code onto a medium such that the code is obtainable  
12                from the medium offline.

1    18.    The offline-online points system of claim 17, wherein the means for  
2                 generating the code includes  
3                 means for providing a number portion,  
4                 means for deriving a validation portion from the number portion,

5 means for appending the validation portion to the number portion to  
6 form a string,  
7 means for encrypting the string, and  
8 means for deriving the code from the encrypted string by converting  
9 the encrypted string to base L string.

1 19. The offline-online points system of claim 18, wherein the code is a fixed-  
2 length string with C characters, and wherein the means for deriving the code further  
3 includes means for prepending a character to the base L string any number of times  
4 that is needed to achieve the fixed-length of C characters.

1 20. The offline-online points system of claim 18, wherein L is the number of  
2 characters in the alphabet.

1 21. The offline-online points system of claim 18, wherein the string is 48-bits  
2 long and the number portion is 32-bits long.

1 22. The offline-online points system of claim 17, wherein the means for  
2 generating the code includes

3 means for providing a number portion,  $S1_{INT}$ , from a first string, S1  
4 means for arranging a first secret key, K1, next to the number  
5 portion,  $S1_{INT}$ , from S1, to form a second string, S2,  
6 means for applying a hash function to S2 to produce a third string,  
7 S3,

8 means for extracting a validation portion,  $S1_{VAL}$ , from S3 and  
9 arranging  $S1_{VAL}$ , next to  $S1_{INT}$  in S1 ( $S1 = S1_{VAL} + S1_{INT}$ ),

10 means for encrypting S1 using a second secret key, K2, to form a  
11 fourth string, S4, and

12 means for deriving the code by converting S4 to a base L fixed-  
13 length code string.

1    23.    The offline-online points system of claim 22, wherein the first and second  
2    secret keys, K1 and K2, are 128-bits long and the encryption means includes DES3  
3    encryption algorithm.

1    24.    The offline-online points system of claim 22, wherein the hash function  
2    application means has MD5, a one-way hash algorithm.

1    25.    The offline-online points system of claim 22, wherein S1 is 48-bits long and  
2    the number portion, S1<sub>INT</sub>, is 32-bits long.

1    26.    The offline-online points system of claim 17, wherein for verifying the  
2    submitted code the code server includes,

3                means for converting the submitted code from a base L string into a  
4                base 2 string, S4<sub>BASE2</sub>,

5                means for decrypting S4<sub>BASE2</sub> using a second secret key, K2, to form a  
6                decrypted first string, S1',

7                means for providing a number portion, S1'<sub>INT</sub>, from S1'

8                means for arranging a first secret key, K1, next to the number  
9                portion, S1'<sub>INT</sub>, from S1, to form a second string, S2',

10              means for applying a hash function to S2' to form a third string S3',

11              means for extracting a validation portion from S3' and a validation portion  
12              from S1', and

13              means for determining if the code is valid by comparing the validation  
14              portion from S3' with the validation portion from S1'.

1    27.    The offline-online points system of claim 26, wherein S3' and S1 are each  
2    48-bits long and the secret keys, K1 and K2 are 128-bits long.

1    28.    The offline-online points system of claim 26, wherein the decryption means  
2    includes DES3<sup>-1</sup> decryption algorithm and the hash function application means  
3    includes MD5 hash algorithm.

1       29. A method for offline-online handling of incentive points, comprising:  
2           generating a code, wherein wherein the code is generated by providing a  
3       number portion, deriving a validation portion from the number portion, appending  
4       the validation portion to the number portion to form a string, encrypting the string,  
5       and deriving the code from the encrypted string by converting the encrypted string  
6       to base L string; and

7           fixing the code onto a medium such that the code is obtainable from the  
8       medium offline.

1       30. The method of claim 29, further comprising:  
2           obtaining the code offline;  
3           submitting the code online to a server that has valid codes, wherein the code  
4       is associated with N points maintained by the server in a user account, wherein each  
5       point, characterized as a purchase or attention incentive point, is redeemable; and  
6           verifying the submitted code against the valid codes to determine if it is  
7       valid, wherein if the submitted code is valid, a predetermined number of points are  
8       added to the user account.

1       31. A method as in claim 29, wherein the code is a fixed-length string with C  
2       characters, and wherein a character is prepended to the base L string any number of  
3       times that is needed to achieve the fixed-length of C characters.

1       32. A method as in claim 29, wherein L is the number of characters in the  
2       alphabet.

1       33. A method as in claim 29, wherein the string is 48-bits long and the number  
2       portion is 32-bits long.

1       34. A method for offline-online handling of incentive points, comprising:  
2           generating a code by:  
3           providing a number portion, S<sub>1<sub>INT</sub></sub>, from a first string, S<sub>1</sub>

4                   arranging a first secret key, K1, next to the number portion, S<sub>1<sub>INT</sub></sub>,  
5                   from S1, to form a second string, S2,  
6                   applying a hash function to S2 to produce a third string, S3,  
7                   extracting a validation portion, S<sub>1<sub>VAL</sub></sub>, from S3 and arranging S<sub>1<sub>VAL</sub></sub>,  
8                   next to S<sub>1<sub>INT</sub></sub> in S1 (S1=S<sub>1<sub>VAL</sub></sub> + S<sub>1<sub>INT</sub></sub> ),  
9                   encrypting S1 using a second secret key, K2, to form a fourth string,  
10                  S4, and  
11                  deriving the code by converting S4 to a base L fixed-length code  
12                  string; and  
13                  fixing the code onto a medium such that the code is obtainable from the  
14                  medium offline.

1       35.   (New) A method as in claim 34, wherein the first and second secret keys,  
2       K1 and K2, are 128-bits long and the encryption involves DES3 encryption  
3       algorithm.

1       36.   A method as in claim 34, wherein the hash function is MD5, a one-way hash  
2       algorithm.

1       37.   (New) A method as in claim 34, wherein S1 is 48-bits long and the number  
2       portion, S<sub>1<sub>INT</sub></sub>, is 32-bits long.

1       38.   (New) A method as in claim 30 wherein the step of verifying the submitted  
2       code includes,  
3                  converting the submitted code from a base L string into a base 2  
4       string, S<sub>4<sub>BASE2</sub></sub>,  
5                  decrypting S<sub>4<sub>BASE2</sub></sub> using a second secret key, K2, to form a decrypted first  
6       string, S1',  
7                  providing a number portion from S1'  
8                  arranging a first secret key, K1, next to the number portion from S1'  
9       to form a second string, S2',  
10                 applying a hash function to S2' to form a third string S3',

11 extracting a validation portion from S3' and a validation portion from S1',  
12 and  
13 determining if the code is valid by comparing the validation portion from S3'  
14 with the validation portion from S1'.

1 39. (New) A method as in claim 38, wherein S3' and S1 are each 48-bits long  
2 and the secret keys, K1 and K2 are 128-bits long.

1 40. (New) A method as in claim 38, wherein the decryption involves DES3<sup>-1</sup>  
2 decryption algorithm and the has function involves MD5 hash algorithm.